UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,183	12/08/2003	Herbert A. Little	555255012471	2882

7590 05/29/2009

David B. Cochran, Esq.
JONES DAY
North Point
901 Lakeside Ave
Cleveland, OH 44114

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
05/29/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/730,183	LITTLE ET AL.	
	Examiner	Art Unit	
	EDWARD ZEE	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) *11-16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 17-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is in respond to the election to restriction filed on January 29th, 2009. Claims 1-32 are pending; Claims 1, 4-7, 10, 24-32 and 2, 3, 8, 9, 17-23 have been elected for examination.

Election/Restrictions

1. Applicant's election **without** traverse of ***Group I:*** *Claims 1, 4-7, 10, 24-32 and 2, 3, 8, 9, 17-23* in the reply filed on January 29th, 2009 is acknowledged. Claims 11-16 have been withdrawn.

Claim Rejections - 35 USC § 112

2. The amendments filed on July 18th, 2008 have been considered and are effective at overcoming the previous claim rejection(s), and thus have been withdrawn.

Claim Rejections - 35 USC § 101

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-10, 17-29 and 31 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-10, 17-29 and 31 disclose a system comprising an authentication information store and an authentication system, which in light of the specification, appear to be software modules. Thus, Claims 1-10, 17-29 and 31 are drawn to software per se. Software is not a series of steps or acts and this is not a process. Software is not a physical article or object and as such is not a machine or manufacture. Software is not a combination of substances and therefore not a compilation of matter. Thus, software by itself

does not fall within any of the four categories of invention. Therefore, Claims 1-10, 17-29 and 31 are not statutory.

The Examiner respectfully notes that, as recited on page 3 of the Applicant's own specification, particular embodiments such as a computer software for performing the method and system of the claimed invention are described, and thus appear to recite at least a purely software embodiment. Therefore, the Examiner respectfully submits that while there may be a recitation of a data store, in light of the specification, the data store appears to encompass software. Furthermore, the data store does not appear to be positively residing on a physical "memory"; nor does the system appear to explicitly comprise of at least a "memory" component or the like.

Claim Rejections - 35 USC § 102

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-10 and 17-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Owen et al. (2004/0187018).

Claim 1: Owen et al. discloses a system for distributing authentication information to users of remote devices comprising:

a. an authentication information store configured to store authentication information for a plurality of users*(ie. record passcode with primary ID 522)* [figure 5];

b. an authentication system configured to receive a request for authentication information for one of the plurality of users from a remote device*(ie. passcode request 508)* [figure 5];

c. wherein the request comprises identity information for use in determining whether the request is from one of the plurality of users*(ie. primary ID, PIN, etc.)* [figure 5];

d. wherein the authentication system retrieves based on the identity information*(ie. primary ID, etc.)* the authentication information for the one of the plurality of users from the authentication information store [figure 5];

e. wherein the retrieved authentication information is provided to the remote device for use in authenticating a user that is requesting remote access to a computer network*(ie. communicate encrypted passcode to the suspect user for presentation to the access authority)* [page 2, paragraph 0010].

Claim 2: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information is used in a two-factor authentication system [figure 1].

Claim 3: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above, and further discloses that the authentication information store comprises a seed store configured to store a plurality of seeds; wherein the authentication system is configured to receive a seed request from the remote device, to retrieve the one of the plurality of seeds from the seed store, to calculate an access code using the retrieved seed, to determine whether the calculated access code matches a received access code and to return the retrieved seed to the remote device where the calculated access code matches the received access

code*(ie. construct rotating key from a shared secret such as a PIN that matches a synchronized server key)* [page 1, paragraph 0007].

Claim 4: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 and further discloses that the request comprises an HTTP connection request [figure 10].

Claim 5: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the request comprises a network password and a digital signature, wherein the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device*(ie. credentials include password and information transmitted from a token of an authorized user)* [page 4, paragraph 0031].

Claim 6: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the identity information comprises user information and account information*(ie. user id, etc.)* [page 4, paragraph 0031].

Claim 7: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 6 above and further discloses that the identity information identifies a particular user and corresponding authentication information being requested, and is used by the authentication system to authenticate the user requesting the authentication information*(ie. compares user ID and respective credentials and/or password etc.)* [page 4, paragraph 0031].

Claim 8: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information in the request is used by the remote device for two-factor authentication [figure 1].

Claim 9: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 8 above and further discloses that the identity information comprises a network password entered by the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the request, a signature key and a signature algorithm*(ie. temporal-based or sequential-based value)* [page 4, paragraph 0031].

Claim 10: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication system does not provide the authentication information to the remote device because a match was not found in the authentication information store based upon the identity information [abstract].

Claim 17: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information comprises a seed from which access codes are to be generated by the remote device, wherein the seed is stored in a protected data store on the remote device*(ie. usb tokens, etc.)* [page 1, paragraph 0007].

Claim 18: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information is used by the remote device to gain access to a corporate local area network(LAN) [figure 10].

Claim 19: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 18 above and further discloses that two-factor authentication is used in the LAN to authenticate a user requesting remote access to the LAN, wherein the retrieved

authentication information is used in performing two-factor authentication in order to gain access to the LAN [figure 10].

Claim 20: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 19 above and further discloses that the retrieved authentication information comprises a seed which the remote device's two-factor code generator uses to produce an access code*(ie. hardware tokens)*;

a. wherein the access code is also based upon a value provided by the remote device's clock, wherein the access code is used by the remote device to gain access to the LAN*(ie. time based token)*;

b. wherein the seed is used by the authentication system to also generate an access code for use in a comparison with the access code generated by the remote device*(ie. synchronized key generated at the server)*;

c. wherein access to the LAN is either granted or denied based upon the comparison [page 1, paragraph 0007].

Claim 21: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 20 above and further discloses that the remote device only generates the access code when access to the LAN is requested by the user of the remote device*(ie. generate passcode after receiving request)* [page 1, paragraph 0010].

Claim 22: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 20 above and further discloses that the authentication information store comprises an index by user name that indicates users authorized for remote access to the

LAN*(ie. authorized users list maintained by the authentication authority)* [page 1, paragraph 0010].

Claim 23: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 22 above and further discloses that the authentication information store stores user seed values form which access codes are to be generated*(ie. synchronized key generated at the server)* [page 1, paragraph 0007].

Claim 24: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device is a wireless mobile communication device [page 2, paragraph 0011].

Claim 25: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 24 above and further discloses that the remote device stores the authentication information in a data store*(ie. usb token)* [page 1, paragraph 0007].

Claims 26 and 27: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 25 above, and further discloses that the data store is implemented in a smart card or USB token(ie. usb token, etc.) [page 1, paragraph 0007].

Claim 28: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device is a desktop computer [page 2, paragraph 0011].

Claim 29: Owen et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device communicates with the authentication system over a communication system, wherein the communication system comprise a wide area network (WAN) and a wireless network gateway [figure 10].

Claim 30: Owen et al. discloses a method for distributing authentication information for remotely accessing computer resources, comprising:

a. receiving a request for the authentication information from a remote device, the request comprising identity information of a user of the remote device*(ie. passcode request 508)* [figure 5];

b. wherein the authentication information is stored in an authentication data store*(ie. record passcode with primary ID 522)* [figure 5];

c. authenticating the user based on the identity information in the request*(ie. primary ID, PIN, etc.)* [figure 5];

d. returning the authentication information to the remote device to authenticate a user requesting remote access to a computer resources based upon the returned authentication information*(ie. communicate encrypted passcode to the suspect user for presentation to the access authority)* [page 2, paragraph 0010].

Claim 31: Owen et al. discloses an apparatus for handling authentication information for users of remote devices, comprising:

a. an authentication information store configured to store authentication information for a user of a remote device, the authentication information provided by a remote authentication system*(ie. record passcode with primary ID 522)* [figure 5];

b. a request for the authentication information from the remote device to the remote authentication system contains identity information*(ie. passcode request 508)* [figure 5];

c. a code generation system configured to retrieve the authentication information*(ie. passcode)* stored in the authentication information store [figure 5];

d. access information*(ie. encrypted passcode is generated from passcode)* is generated based upon the retrieved authentication information and is used to authenticate a user requesting remote access to a remote computer network [figure 5].

Claim 32: Owen et al. discloses a method for obtaining authentication information for remotely accessing a computer network, comprising:

a. providing a request from a user of a remote device to an authentication system for the authentication information that is stored in a data store by the authentication system*(ie. passcode request 508)* [figure 5];

b. the request comprises identity information*(ie. primary ID, etc.)* for use by the authentication system to authenticate the user based on the identity information provided in the request [figure 5];

c. receiving by the remote device the authentication information from the authentication system*(ie. communicate encrypted passcode to the suspect user for presentation to the access authority)* [page 2, paragraph 0010];

d. wherein the received authentication information is used to authenticate a user requesting remote access to the computer network*(ie. presentation to the access authority)* [page 2, paragraph 0010].

Response to Arguments

6. Applicant's arguments filed July 18th, 2008 have been fully considered but they are not persuasive.

Regarding Claim 1: The Applicant argues that Owen et al. does not disclose authentication information retrieved from a data store that is sent to the remote device, and in particular notes that Owen et al. does not retrieve the "encrypted passcode" from a data store. Furthermore, the Applicant submits that because the passcode disclosed by Owen et al. is in fact generated in respond to a request, it cannot be a pre-existing passcode.

However, the Examiner respectfully submits that the instant claim as currently recited does not appear to require an authentication information which is expressly "pre-generated" and/or "pre-stored", per se. Thus, a "generated passcode", as disclosed by Owen et al., would fairly suggest that it would have to be stored on some form of memory(ie. volatile memory such as RAM, cache, etc.) after it is generated and before it is transmitted to the remote device.

Furthermore, the Examiner notes that the Applicant's own specification appears to suggest "dynamically" generated authentication information as well [page 29, lines 15-19].

Therefore, the Examiner respectfully disagrees and submits that, in light of the discussion above, Owen et al. does in fact appear to teach the allegedly deficient limitations.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies *(i.e., "pre-stored/pre-generated" authentication information or the like)* are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to EDWARD ZEE whose telephone number is (571)270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
May 13, 2009
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435